Payment Card Industry
Data Security Standard

Attestation of Compliance for Self-Assessment Questionnaire P2PE

For use with PCI DSS Version 4.0

Publication Date: April 2022

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the merchant's self-assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures.* Complete all sections. The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which the Attestation of Compliance (AOC) will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Self-Assessment Questionnaire (SAQ).

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Self-Assessment Questionnaire.

Part 1. Contact Information	
Part 1a. Assessed Merchant	
Company name:	
DBA (doing business as):	
Company mailing address:	
Company main website:	
Company contact name:	
Company contact title:	
Contact phone number:	
Contact e-mail address:	
Part 1b. Assessor	
Provide the following information for all assessors involved in the assessment. If there was no assessor for a given assessor type, enter Not Applicable.	
PCI SSC Internal Security Assessor(s)	
ISA name(s):	
Qualified Security Assessor	
Company name:	
Company mailing address:	
Company website:	
Lead Assessor Name:	
Assessor phone number:	
Assessor e-mail address:	
Assessor certificate number:	

Part 2. Executive Summary

Part 2a. Merchant Business Payment Channels (select all that apply):

Indicate all payment channels used by the business that are included in this assessment.

☐ Mail order/telephone order (MOTO)
☐ Card-present

Are any payment channels not included in this assessment? If yes, indicate which channel(s) is not included in the assessment and provide a brief explanation about why the channel was excluded.	☐ Yes ☐ No

Note: *If the organization has a payment channel that is not covered by this SAQ, consult with the entity(ies) to which this AOC will be submitted about validation for the other channels.*

Part 2b. Description of Role with Payment Cards

For each payment channel included in this assessment as selected in Part 2a above, describe how the business stores, processes and/or transmits account data.

Channel	How Business Stores, Processes, and/or Transmits Account Data

Part 2c. Description of Payment Card Environment

Provide a ***high-level*** description of the environment covered by this assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.* • *System components that could impact the security of account data.*	
Indicate whether the environment includes segmentation to reduce the scope of the assessment. *(Refer to "Segmentation" section of PCI DSS for guidance on segmentation.)*	☐ Yes ☐ No

Part 2. Executive Summary *(continued)*

Part 2d. In-Scope Locations/Facilities

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers, and mail rooms) in scope for the PCI DSS assessment.

Facility Type	Total number of locations (How many locations of this type are in scope)	Location(s) of facility (city, country)
Example: Data centers	*3*	*Boston, MA, USA*

Part 2e. PCI Validated P2PE Solution

Provide the following information regarding the validated♦ PCI-listed P2PE solution used by the merchant:

Name of P2PE Solution Provider:	
Name of P2PE Solution:	
P2PE Solution listing "Reference #":	
Listed POI Devices used by Merchant (found under "PTS POI Devices Supported"):	
P2PE Solution "Reassessment Date":	

♦ *P2PE solutions on the PCI list of Point-to-Point Solutions with Expired Validations are no longer considered "validated" per the P2PE Program Guide. Merchants using an expired P2PE solution should check with their acquirer or individual payment brands about acceptability of this SAQ.*

Part 2. Executive Summary *(continued)*

Part 2f. Third-Party Service Providers

Does the merchant have relationships with one or more third-party service providers that:

• Store, process, or transmit account data on the merchant's behalf (for example, payment gateways, payment processors, payment service providers (PSPs), and off-site storage)	☐ Yes ☐ No
• Manage system components included in the scope of the merchant's PCI DSS assessment—for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting services, and IaaS, PaaS, SaaS, and FaaS cloud providers.	☐ Yes ☐ No
• Could impact the security of the merchant's CDE (for example, vendors providing support via remote access, and/or bespoke software developers)	☐ Yes ☐ No

If Yes:

Name of service provider:	**Description of service(s) provided:**

Note: *Requirement 12.8 applies to all entities in this list.*

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment
(SAQ Section 2 and related appendices)

Indicate below all responses that were selected for each PCI DSS requirement.

PCI DSS Requirement *	Requirement Responses *More than one response may be selected for a given requirement. Indicate all responses that apply.*				
	In Place	In Place with CCW	In Place with Remediation	Not Applicable	Not in Place
Requirement 3:	☐	☐	☐	☐	☐
Requirement 9:	☐	☐	☐	☐	☐
Requirement 12:	☐	☐	☐	☐	☐

** PCI DSS Requirements indicated above refer to the requirements in Section 2 of the SAQ associated with this AOC.*

Part 2h. Eligibility to Complete SAQ P2PE

Merchant certifies eligibility to complete this Self-Assessment Questionnaire because, for this payment channel:

☐	All payment processing is via a validated PCI-listed P2PE solution (per Part 2e above).
☐	The only systems in the merchant environment that store, process or transmit account data are the payment terminals that are part of the validated* PCI-listed P2PE solution.
☐	The merchant does not otherwise receive, transmit, or store account data electronically.
☐	Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically**;**
☐	The merchant has implemented all controls in the P2PE Instruction Manual (PIM) provided by the P2PE Solution Provider.

Section 2: Self-Assessment Questionnaire P2PE

Self-assessment completion date:	YYYY-MM-DD
Were any requirements in the SAQ unable to be met due to a legal constraint?	☐ Yes ☐ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ P2PE (Section 2), dated (Self-assessment completion date *YYYY-MM-DD).*

Based on the results documented in the SAQ P2PE noted above, each signatory identified in any of Parts 3b–3d, as applicable, assert(s) the following compliance status for the merchant identified in Part 2 of this document.

Select one:

☐	**Compliant:** All sections of the PCI DSS SAQ are complete and all requirements are marked as being either 1) In Place, 2) In Place with Remediation, or 3) Not Applicable, resulting in an overall **COMPLIANT** rating; thereby *(Merchant Company Name)* has demonstrated compliance with all PCI DSS requirements included in this SAQ.
☐	**Non-Compliant:** Not all sections of the PCI DSS SAQ are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *(Merchant Company Name)* has not demonstrated compliance with the PCI DSS requirements included in this SAQ. **Target Date** for Compliance: *YYYY-MM-DD* A merchant submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted *before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more requirements in the PCI DSS SAQ are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other requirements are marked as being either 1) In Place, 2) In Place with Remediation, or 3) Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Merchant Company Name)* has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not in Place due to a legal restriction. This option requires additional review from the entity to which this AOC will be submitted. *If selected, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement from being met

Part 3a. Merchant Acknowledgement

Signatory(s) confirms:

(Select all that apply)

☐	PCI DSS Self-Assessment Questionnaire P2PE, Version 4.0, was completed according to the instructions therein.
☐	All information within the above-referenced SAQ and in this attestation fairly represents the results of the merchant's assessment in all material respects.
☐	PCI DSS controls will be maintained at all times, as applicable to the merchant's environment.

Part 3b. Merchant Attestation

Signature of Merchant Executive Officer ↑	*Date: YYYY-MM-DD*
Merchant Executive Officer Name:	*Title:*

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this assessment, indicate the role performed:	☐ QSA performed testing procedures.
	☐ QSA provided other assistance. If selected, describe all role(s) performed:

Signature of Lead QSA ↑	*Date: YYYY-MM-DD*
Lead QSA Name:	

Signature of Duly Authorized Officer of QSA Company ↑	*Date: YYYY-MM-DD*
Duly Authorized Officer Name:	*QSA Company:*

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☐ ISA(s) provided other assistance. If selected, describe all role(s) performed:

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has a Non-Compliant status noted in Section 3.

If asked to complete this section, select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement below. For any "No" responses, include the date the merchant expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

PCI DSS Requirement*	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
3	Protect stored account data	☐	☐	
9	Restrict physical access to cardholder data.	☐	☐	
12	Support information security with organizational policies and programs	☐	☐	

** PCI DSS Requirements indicated above refer to the requirements in Section 2 of the SAQ associated with this AOC.*